IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF MISSOURI
WESTERN DIVISION

Ronald M. Celestine, on behalf of himself and all others similarly situated, Plaintiff, v. Uber Technologies, Inc., Defendant.	CASE NO. **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Ronald M. Celestine ("Plaintiff"), individually and on behalf of the similarly situated persons defined below, alleges the following against Uber Technologies, Inc. ("Uber" or "Defendant"). Plaintiff makes these allegations upon personal knowledge with respect to himself and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters.

NATURE OF THE ACTION

1. Plaintiff brings this class action against Uber for its failure to secure and safeguard the private information of approximately 57 million riders and drivers who use its service and for Uber's concealment and refusal to provide notification for over a year to individuals affected by the data breach.

2. On November 21, 2017, Uber publicly announced that in October 2016 hackers accessed Uber user data stored on a third-party cloud-based service (the "2016 Security Breach"). The 2016 Security Breach disclosed the personal information of approximately 57 million users, including 600,000 U.S. drivers. The personal information disclosed included names, email addresses, private cell phone numbers, and driver's license information for drivers

(the "Personal Information"). Uber then paid the hackers $100,000 in exchange for their assurance that they would delete the data.

3. The 2016 Security Breach was caused by Uber's reckless violation of its obligations to secure the Personal Information entrusted to it. Uber failed to comply with security standards and allowed the private information of millions collected by Uber to be compromised.

4. Accordingly, Plaintiff, on behalf of himself and all others similarly situated, asserts claims for negligence, breach of contract, and for violation of California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq.* ("UCL").

PARTIES

5. Plaintiff Ronald M. Celestine is an individual and a citizen of Kansas, who drove for Defendant Uber Technologies, Inc. in 2015. Plaintiff was engaged as a driver for Uber in Kansas City, Missouri, and operated as an Uber driver in Missouri. On information and belief, Plaintiff's Personal Information, including his driver's license information, cell phone number, name, and email address were compromised in the 2016 Security Breach.

6. Defendant Uber Technologies, Inc. is a global transportation company operated in over 600 cities worldwide. Defendant is a Delaware corporation with its principal place of business at 800 Market Street, 7th Floor, San Francisco, CA 94102. Defendant is registered to do business in Missouri and can be served through its registered agent, CT Corporation System, 120 South Central Avenue, Clayton, MO 63015.

JURISDICTION AND VENUE

7. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d)(2), in that the matter is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, and members of the Class are citizens of states different from Defendant.

8. This Court has personal jurisdiction over Defendant because it maintains or has maintained an office and conducts business in this district.

9. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(1) and (c)(2) because Defendant is a resident of this District, and under 28 U.S.C. § 1391(b)(2) because a substantial part of the events and omissions giving rise to this action occurred in this District.

FACTUAL BACKGROUND

10. Plaintiff brings this class action against Uber for its failure to secure and safeguard his Personal Information, and that of similarly situated people who either drove for Uber or used its services as riders, and for failing to timely and adequately notify Plaintiff and other Class members that their Personal Information had been stolen and of what types of information was stolen.

11. Uber develops, markets, and operates a mobile-app-based transportation network called Uber. The Uber app allows riders to submit a trip request on their smartphone, which is routed to Uber's drivers.

12. Uber's business depends on drivers, who must provide extensive identifying information, including extremely sensitive information such as Social Security Numbers, to Uber in order to work as drivers and earn a livelihood.

13. Riders also must provide Personal Information in order to use Uber's services, including financial information that is required to pay for rides through Uber's app.

A. Uber Failed to Notify Drivers and Riders About a Massive Data Breach in 2016, Instead Paying the Hackers to Hide It.

14. On November 21, 2017, news reports were published that made it public, for the first time, that Uber suffered a massive data breach in October 2016, in which the Personal Information of some 57 million of Uber's riders and drivers was accessed by hackers.[1]

15. In December 2017, it was revealed that the hack was accomplished by a 20-year-old Florida man with the help of an individual in Canada.[2]

---

[1] *See, e.g.,* <https://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data> (last visited March 20, 2018).

[2] *See* <https://www.reuters.com/article/us-uber-cyber-payment-exclusive/exclusive-uber-paid-20-year-old-florida-man-to-keep-data-breach-secret-sources-idUSKBN1E101C> (last visited March

16. Uber learned about the 2016 Security Breach by November 2016, but purposely chose not to notify those whose Personal Information was compromised at that time.

17. Instead of notifying the victims of the 2016 Security Breach about it, Uber paid the hackers who perpetrated it $100,000 through a so-called "bug bounty" program normally used to identify small code vulnerabilities, in an effort to cover it up.[3] Uber thus conspired with the hackers who perpetrated the 2016 Security Breach to keep its victims — Uber's drivers and riders — in the dark.

18. According to the news reports, the 2016 Security Breach occurred when the two hackers "accessed a private GitHub coding site used by Uber software engineers and then used login credentials they obtained there to access data stored on an Amazon Web Services account that handled computing tasks for the company. From there, the hackers discovered an archive of rider and driver information. Later, they emailed Uber asking for money, according to the company."[4]

19. "Compromised data from the October 2016 attack included names, email addresses and phone numbers of 50 million Uber riders around the world . . . . The personal information of about 7 million drivers was accessed as well, including some 600,000 U.S. driver's license numbers."[5]

20. According to these news reports, Uber's board of directors commissioned an investigation into the activities of its security team in or around October 2017, which team was led by Uber's Chief Security Officer, Joe Sullivan. This project, conducted by an outside law firm, discovered the 2016 Security Breach and the failure to disclose it.[6]

20, 2018); <https://www.reuters.com/article/us-uber-cyber-congress/uber-says-hackers-behind-2016-data-breach-were-in-canada-florida-idUSKBN1FQ2YO> (last visited March 20, 2018).

[3] *Id.*

[4] *Id.*

[5] *Id.*

[6] *Id.*

21. In response to this discovery, Dara Khosrowshahi, who has been Uber's CEO since August 2017, asked for the resignation of Mr. Sullivan and fired Craig Clark, a senior lawyer who reported to Mr. Sullivan.[7]

22. On February 6, 2018, Uber's chief information security officer, John Flynn, testified before the Senate Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security that Uber had "no justification" for not notifying the public sooner about the breach, and admitted that "it was wrong not to disclose the breach earlier."[8]

23. As these news reports surfaced, Uber published several statements concerning the 2016 Security Breach on its own website, confirming much of what was published in the news reports.

24. According to one of Uber's statements concerning the 2016 Security Breach, driver information "included the names, email addresses and mobile phone numbers related to accounts globally. In addition, the driver's license numbers of around 600,000 drivers in the United States were downloaded."[9]

25. Uber has yet to provide any direct notification to victims of the 2016 Security Breach that their Personal Information was compromised.

B. Uber Also Failed to Notify Class Members About a Similar 2014 Security Breach.

26. At the time Uber discovered the 2016 Security Breach and made the illegal and immoral decision not to disclose it, Uber had recently settled a lawsuit with the New York Attorney General over a very similar data breach that occurred in 2014 (the "2014 Security Breach"), and was in the process of negotiating with the Federal Trade Commission over its handling of consumer data.

---

[7] *Id.*

[8] *See* <https://arstechnica.com/tech-policy/2018/02/uber-we-had-no-justification-for-covering-up-data-breach/> (last visited March 20, 2018).

[9] *See* <https://help.uber.com/h/0ded7de4-ed4d-4c75-a3ee-00cddeafc372> (last visited March 20, 2018).

27. In the 2014 Security Breach, much like the 2016 Security Breach, one or more hackers utilized credentials that Uber made available on one or more GitHub webpages (and/or via the GitHub app, which is an app designed for sharing code among app developers).[10]

28. Uber did not disclose the 2014 Security Breach until February 27, 2015, when it disseminated a Press Release stating, *inter alia*, "In late 2014, we identified a one-time access of an Uber database by an unauthorized third party. . . ." (the "2015 Press Release").

29. Uber admitted in its 2015 Press Release that it knew of the 2014 Security Breach at least as early as September 17, 2014 — over five months before Uber issued the 2015 Press Release or made any effort whatsoever to notify those affected that their Personal Information had been disclosed.

30. Uber's 2015 Press Release further stated that "unauthorized access to an Uber database by a third party . . . occurred on May 13, 2014," and that "the unauthorized access impacted approximately 50,000 drivers across multiple states."

31. At approximately the same time it issued its 2015 Press Release, Uber also issued notifications to victims of the 2014 Security Breach, which included substantially the same information and which informed recipients that their name and driver's license numbers had been disclosed in the breach.

32. Uber's initial representations about the 2014 Security Breach indicated, much as its current representations concerning the 2016 Security Breach indicate, that only driver's license numbers and names were disclosed in the 2014 Security Breach. However, this turned out to be false.

33. In or around August 2016 — approximately two years after the 2014 Security Breach, and shortly before Uber's discovery of the 2016 Security Breach — Uber issued more notifications to victims of the 2014 Security Breach informing them that, contrary to its earlier representations and notices, additional Personal Information was disclosed in the 2014 Security

[10] *See, e.g.*, <https://www.bloomberg.com/news/articles/2017-11-22/uber-hack-shows-vulnerability-of-software-code-sharing-services> (last visited March 20, 2018).

Breach. In fact, contrary to its initial representations concerning the scope of the 2014 Security Breach, additional Personal Information was disclosed in the 2014 Security Breach, including banking information and Social Security Numbers, in addition to driver's license numbers and names.

C. Plaintiff Has Been Injured by the 2016 Security Breach.

34. Uber has repeatedly disregarded Plaintiff's and Class members' rights by intentionally, willfully, and recklessly failing to take adequate and reasonable measures to ensure its data systems were protected, failing to take available steps to prevent and stop the 2016 Security Breach from ever happening, despite its experience with the 2014 Security Breach (which both occurred because Uber made credentials available through GitHub websites), and failing to disclose to those affected the facts that it did not have adequate computer systems and security practices in place, and that the 2016 Security Breach had occurred, in a timely manner. On information and belief, Plaintiff's and Class members' Personal Information and the password allowing access to that Personal Information were improperly handled and stored, were unencrypted, and were not kept in accordance with applicable, required, and appropriate cyber-security protocols, policies, and procedures. As a result, Plaintiff's and Class members' Personal Information was compromised and stolen.

35. Disclosure of the types of Personal Information that Uber admits were compromised in the 2016 Security Breach presents a danger to victims of the breach. Information such as data breach victims' names, email addresses, and other identifying information *alone* creates a material risk of identity theft. Identity thieves can use such personal information to locate additional personal information, such as financial information and Social Security Numbers, and use the combined information to perpetrate fraud such as, for instance, opening new financial accounts in victims' names, or filing false tax returns in victims' names and collecting the tax refunds.

36. In addition, given the facts surrounding the 2014 and 2016 Security Breaches, Uber's current representations concerning the scope of the 2016 Security Breach cannot be

accepted as true. Uber possesses a wide variety of personal information concerning Class members, and repeatedly has failed to protect that personal information. Based on the facts alleged above, Plaintiff believes that all the personal information that Uber has about him has been handled incompetently and improperly, and Plaintiff must assume that all of the personal information in Uber's possession has been obtained by hackers who either will misuse that personal information themselves or sell it to others who will do so, if this has not already occurred. There is no expiration on how long victims' personal information can stay in the hands of identity thieves before it is misused.

37. Plaintiff and other Class members suffered injuries including but not limited to time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, invasion of their privacy, and loss of value of their Personal Information.

38. It is well known and the subject of many media reports that Personal Information like that taken in the 2016 Security Breach is highly coveted and a frequent target of hackers.

39. Legitimate organizations and the criminal underground alike recognize the value in such Personal Information. Otherwise, they would not pay for it or aggressively seek it.

40. "Increasingly, criminals are using biographical data gained from multiple sources to perpetrate more and larger thefts."[11]

41. The ramifications of Uber's failure to keep Class members' data secure are severe.

42. There is a strong likelihood that Class members will become victims of identity fraud in the future given the breadth of their Personal Information that is now available to identity thieves and other criminals on the dark web.

[11] Verizon 2014 PCI Compliance Report, *available at* <http://www.cisco.com/c/dam/en_us/solutions/industries/docs/retail/verizon_pci2014.pdf> (hereafter "2014 Verizon Report"), at 54 (last visited March 20, 2018).

43. As the FTC recognizes, once identity thieves have Personal Information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[12]

44. Identity thieves can use Personal Information such as that of Class members, which Uber failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund. Some of this activity may not come to light for years.

45. In addition, identity thieves can commit any number of other frauds, such as obtaining a job, procuring housing, or even giving false information to police during an arrest.

46. Plaintiff and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such injuries.

47. Uber's wrongful actions and inactions directly and proximately caused the theft and dissemination into the public domain of Plaintiff's and Class members' Personal Information, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. theft of their Personal Information;

b. the untimely and inadequate notification of the 2016 Security Breach;

c. loss of privacy;

[12] FTC, Warning Signs of Identity Theft, *available at* <http://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft> (last visited March 20, 2018).

d. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the 2016 Security Breach;

e. deprivation of rights they possess under California law, including the Business and Professions Code § 17200, *et seq*.

CLASS ACTION ALLEGATIONS

48. Plaintiff seeks relief in his individual capacity and as a representative of all others who are similarly situated. In accordance with Fed. R. Civ. P. 23(a) and (b)(2) and/or (b)(3), Plaintiff seeks certification of the following class (the "Class"):

> All persons residing in the United States whose personal information was disclosed in the data breach affecting Uber Technologies, Inc. in 2016.

49. Excluded from the Class are Defendant, including any entity in which Defendant has a controlling interest, is a parent or subsidiary, or which is controlled by Defendant, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Defendant. Also excluded are the judges and court personnel in this case and any members of their immediate families.

50. Numerosity. Fed. R. Civ. P. 23(a)(1). The members of the Class are so numerous that the joinder of all members is impractical. While the exact number of Class members is unknown to Plaintiff at this time, based on Defendant's statements, Personal Information pertaining to approximate 57 million riders and drivers, globally, was disclosed in the 2016 Security Breach. According to statements from Uber's chief information security officer, John Flynn, about 25 million of the individuals affected were in the United States.[13]

[13] *See* <http://thehill.com/policy/technology/372596-uber-no-justification-for-covering-up-data-breach> (last visited March 19, 2018).

51. Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3). There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

a. Whether Defendant owed a duty to Plaintiff and members of the Class to adequately protect their Personal Information and to provide timely and accurate notice of the 2016 Security Breach to Plaintiff and members of the Class;

b. Whether Defendant knew or should have known that its systems were vulnerable to attack;

c. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of tens of thousands of individuals' Personal Information;

d. Whether Defendant's Personal Information storage and protection protocols were reasonable and compliant with industry standards;

e. Whether Class members may obtain injunctive relief against Defendant under the UCL;

f. Whether Defendant has an express or implied contractual obligation to use reasonable security measures;

g. Whether Defendant complied with any express or implied contractual obligation to use reasonable security measures;

h. Whether Defendant violated California Business and Professions Code § 17200, *et seq.*;

i. Whether Plaintiff and members of the Class are entitled to recover actual damages; and

j. Whether Plaintiff and members of the Class are entitled to equitable relief, including injunctive relief, restitution, and disgorgement.

52. Ascertainability. All members of the purposed Class are readily ascertainable. Defendant has access to addresses and other contact information for all, or substantially all, members of the Class, which can be used for providing notice to many Class members.

53. Typicality. Fed. R. Civ. P. 23(a)(3). Plaintiff's claims are typical of those of other Class members because Plaintiff's information, like that of every other Class member, was misused and/or disclosed by Defendant.

54. Adequacy of Representation. Fed. R. Civ. P. 23(a)(4). Plaintiff will fairly and adequately represent and protect the interests of the members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions, including class actions involving data breaches.

55. Superiority of Class Action. Fed. R. Civ. P. 23(b)(3). A class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Class is impracticable. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

56. Damages for any individual Class member are likely insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendant's violations of law inflicting substantial damages in the aggregate would go un-remedied without certification of the Class.

57. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2), because Defendant has acted or has refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

COUNT I

Negligence

(On Behalf of Plaintiff and the Class)

58. Plaintiff incorporates the substantive allegations above as if fully set forth herein.

59. Defendant owed a duty to Plaintiff and Class members, who were required to provide their Personal Information to Defendant in order to get paid for their work as Uber drivers or to access its riding services, arising from the sensitivity of the Personal Information and the foreseeability of the 2016 Security Breach and of Defendant's data security shortcomings, to exercise reasonable care in safeguarding their Personal Information. This duty included, among other things, designing, maintaining, implementing, monitoring, testing, and complying with reliable security systems, protocols, and practices to ensure that Class members' information was adequately secured from unauthorized access.

60. Defendant owed a duty to Class members to implement cybersecurity systems and processes that would detect a data breach in a timely manner, and not allow Personal Information or keys that would access Personal Information to be published or otherwise made available to identity thieves.

61. Defendant also had a duty to delete any Personal Information that was no longer needed to serve its drivers' and riders' needs, and not use former drivers' or riders' Personal Information in the conduct of its business going forward.

62. Defendant also owed a duty to Class members to notify them promptly that their Personal Information was compromised in the 2016 Security Breach.

63. Defendant breached its duties by, among other things: (a) failing to implement and maintain adequate data security practices to safeguard Class member' Personal Information; (b) failing to detect the 2016 Security Breach in a timely manner; (c) failing to notify Class members promptly and with full information concerning the 2016 Security Breach; and (d) failing to disclose that Defendant's data security practices were inadequate to safeguard Class members' Personal Information.

64. But for Defendant's breach of its duties, Class members' Personal Information would not have been compromised in the 2016 Security Breach.

65. Plaintiff and Class members were foreseeable victims of Defendant's inadequate data security practices. Defendant knew or should have known that a breach of its data security systems would cause damages to Class members.

66. As a result of Defendant's negligent and/or willful failure to prevent the 2016 Security Breach, Plaintiff and Class members suffered injury, which includes but is not limited to lost benefit of their bargain with Defendant; exposure to a heightened, imminent risk of fraud; identity theft; and financial harm. Plaintiff and Class members must more closely monitor their financial accounts and credit histories to guard against identity theft and misuse of their Personal Information. Class members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized release of Plaintiff's and Class members' Personal Information also diminished the value of that Personal Information.

67. The damages to Plaintiff and other Class members were a proximate, reasonably foreseeable result of Defendant's breaches of its duties.

68. Plaintiff and Class members are entitled to damages in an amount to be proven at trial.

COUNT II

Breach of Contract

(On Behalf of Plaintiff and the Class)

69. Plaintiff incorporates the substantive allegations above as if fully set forth herein.

70. Defendant entered into a contract with Plaintiff and Class members, which includes terms covering privacy and limiting the use and sharing of Plaintiff's and Class members' Personal Information.

71. Plaintiff and Class members bargained for an adequate level of security and reasonable care with respect to the use, storage, and sharing of their Personal Information.

72. Plaintiff and Class members performed their duties under the contract.

73. Defendant violated the terms of the contract in the 2016 Security Breach by sharing Plaintiff's and Class members' Personal Information for unauthorized purposes, without first obtaining Plaintiff's and Class members' consent or anonymizing and/or aggregating the information in a form which cannot reasonably be used to identify them, and otherwise violating the terms of the contract.

74. Defendant violated the terms of the contract in the 2016 Security Breach by failing to take appropriate measures to protect Plaintiff's and Class members' Personal Information in accordance with its promises and representations. Defendant violated the contract by failing to comply with applicable laws during the 2016 Security Breach regarding the access, correction, and/or deletion of Personal Information, and notification to affected persons.

75. Plaintiff and Class members have suffered actual damages which include but are not limited to lost benefit of their bargain with Defendant; exposure to a heightened, imminent risk of fraud; identity theft; and financial harm. Plaintiff and Class members must more closely monitor their financial accounts and credit histories to guard against identity theft and misuse of their Personal Information. Class members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized release of Plaintiff's and Class members' Personal Information also diminished the value of that Personal Information.

COUNT III

Violation of California Unfair Competition Law, Bus. & Prof. Code § 17200, *et seq*.

(On Behalf of Plaintiff and the Class)

76. Plaintiff incorporates the substantive allegations above as if fully set forth herein.

77. Defendant from its headquarters in California engaged in unfair, fraudulent and unlawful business practices in violation of the Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq.* ("UCL").

78. Plaintiff suffered injury in fact and lost money or property as a result of Defendant's violations of the UCL.

79. The acts, omissions, and conduct of Defendant as alleged constitutes a "business practice" within the meaning of the UCL.

80. Defendant's acts, omissions, and conduct violate the unfair prong of the UCL because those acts, omissions, and conduct, as alleged herein, offended public policy and constitute immoral, unethical, oppressive, and unscrupulous activities that caused substantial injury, including to Plaintiff and other Class members. The harm cause by Defendant's conduct outweighs any potential benefits attributable to such conduct and there were reasonably available alternatives to further Defendant's legitimate business interests, other than Defendant's conduct described herein.

81. Defendant's conduct also undermines California public policy — as reflected in statutes like the Information Practices Act, Cal. Civ. Code § 1798 *et seq.*, and the California Customer Records Act, Cal. Civ. Code §§ 1798.81.5 and 1798.82 concerning customer records — which seek to protect customer data and ensure that entities who solicit or are entrusted with personal data utilize reasonable security measures.

82. By failing to disclose that it does not enlist industry standard security practices, which render Defendant's app and services particularly vulnerable to data breaches, Defendant engaged in a fraudulent business practice that is likely to deceive a reasonable consumer.

83. A reasonable person would not have agreed to use the Uber app or to act as an Uber driver had he or she known the truth about Defendant's security procedures. By withholding material information about its security practices, Defendant was able to convince drivers and riders to provide and entrust their Personal Information to Defendant.

84. Defendant's failure to disclose that it does not enlist industry standard security practices also constitutes an unfair business practice under the UCL. Defendant's conduct is unethical, unscrupulous, and substantially injurious to Class members.

85. As a result of Defendant's violations of the UCL, Plaintiff and the other Class members are entitled to injunctive relief including, but not limited to: (1) ordering that Defendant utilize strong industry standard encryption algorithms for encryption keys that provide access to stored Personal Information; (2) ordering that Defendant implement the use of its encryption keys in accordance with industry standards; (3) ordering that Defendant, consistent with industry standard practices, engage third party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests and audits on Defendant's systems on a periodic basis; (4) ordering that Defendant engage third party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring; (5) ordering that Defendant audit, test and train its security personnel regarding any new or modified procedures; (6) ordering that Defendant, consistent with industry standard practices, segment Personal Information by, among other things, creating firewalls and access controls so that if one area of Defendant's computer system is compromised, hackers cannot gain access to other portions of its systems; (7) ordering that Defendant purge, delete, and destroy in a reasonably secure manner Personal Information not necessary for its provisions of services; (8); ordering that Defendant, consistent with industry standard practices, conduct regular database scanning and security checks; (9) ordering that Defendant, consistent with industry standard practices, evaluate smartphone and web applications for vulnerabilities to prevent threats to drivers and other users of the Uber app; (10) ordering that Defendant, consistent with industry standard practices, periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; (11) ordering that Defendant stop using GitHub or allowing Personal Information to be accessed with single credentials; and (12) ordering Defendant to meaningfully educate its drivers and riders about the threats they face as a result of the loss of

their Personal Information to third parties, as well as the steps they must take to protect themselves.

86. As a result of Defendant's violations of the UCL, Plaintiff and other Class members have suffered injury in fact and lost money or property, as detailed above. Plaintiff requests that the Court issue sufficient equitable relief to restore Class members to the position they would have been in had Defendant not engaged in unfair competition, including by ordering restitution of all funds that Defendant acquired as a result of its unfair competition, including fees that Defendant retained for rides given by Plaintiff and for rides given by and to other Class members.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all Class members proposed in this Complaint, respectfully request that the Court enter judgment in their favor and against Defendant, as follows:

A. For an Order certifying this action as a class action and appointing Plaintiff and his Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class members' Personal Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class members;

C. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

D. For an award of actual and compensatory damages in an amount to be determined;

E. For an award of costs of suit as allowable by law; and

F. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands trial by jury of all claims so triable.

Dated: March 20, 2018

Respectfully submitted,

/s/ Norman E. Siegel

Norman E. Siegel, MO# 44378
Barrett J. Vahle, MO# 56674
Lindsay Todd Perkins, MO# 60004
J. Austin Moore, MO# 64040
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
Phone: (816) 714-7100
Fax: (816) 714-7101
siegel@stuevesiegel.com
vahle@stuevesiegel.com
perkins@stuevesiegel.com
moore@stuevesiegel.com

Counsel for Plaintiff